Discussion paper: The relationship between biometrics and artificial intelligence (AI)

Exploring the intersection between biometrics and AI

Version 5 as at 23 April 2024

Introduction

Over the past year, the opportunities and challenges of AI and biometrics have delivered many headlines and a need to clarify what policies and legislation will need to be put in place to ensure the responsible use of these technologies. The very first question the Institute members have identified is whether all biometric uses are AI. Many believe that is not the case and the two should be separated. Therefore, an explanation (and definition) of the relationship of biometrics and AI is critical to understand how policy and legislation will apply to biometrics.

The Institute is therefore releasing a discussion paper untangling the issues and putting them to its global membership for debate. The output will be a new entry to the *Biometrics Institute Explanatory Dictionary* as well as briefings to members, policy makers and regulators on the findings and viewpoints.

From April to June 2024, we will take this discussion into the upcoming Biometrics Institute conferences:

- ID@Borders on the 18-19 April in Helsinki will have a first working group meeting that members can join in person to have a first conversation about the issues.
- Asia-Pacific Conference on the 22-23 May in Sydney will have a panel of experts engaging with the audience to collect viewpoints from the region.
- US Strategy Forum on the 20 June in Washington DC will have a similar panel of experts engaging with the audience.
- An On the Pulse Conversation in an online format will then be scheduled between July and September to allow our global audience to join in.
- The Congress in London on the 22-23 October is going to look at the findings followed by the Showcase Australia on the 4 December in Canberra.

We are going to ask the following questions based on the discussion paper:

- How would you define the relationship between AI and biometrics: Are biometrics to be subset of AI or is AI to be a subset of biometrics?
- Biometrics & AI: What are the corresponding issues?
- How does AI interact with biometrics: is there a relatively small overlap between the two or are they completely separate?

How can you comment?
If you have a view on what the relationship between AI and biometrics is, then you are encouraged to join this important conversation to help shape the output that we will use to better inform decision-makers. Please note that only members of the Biometrics Institute can make contributions and due to the limited resources we have available we can only accept written contributions that use this paper and mark it up with proposed changes to the questions below.

Note to reader: All these statements and examples are illustrations of things that can happen or uses that may be seen in public discourse, not definitions of things that do happen in every instance or are considered correct by every stakeholder. This paper should be read in conjunction with several entries in the *Explanatory Dictionary of Biometrics* – to which we will add that for Artificial Intelligence (AI), see the attachment to this paper for a first draft of this entry. You may also wish to review the slides we have created that illustrate the questions further. They can be found in the annex to this paper.

1. The challenge of defining the relationship between AI and biometrics

1.1 Relationships in usage and the biometrics and AI hierarchy

The term AI and its various interpretations
AI usually means something like 'machine performance of a function or computation that might ordinarily be considered like human mental processes'. In this framing, function means 'a thing done by the machine that can be observed from the outside' (e.g., production of an image from a user-supplied description); and computation means 'a thing done by the machine that forms part of its internal workings' (e.g., use of a neural network to process some internal data, unseen from the outside).

The term AI may therefore be variously interpreted as:

a. the specific use of techniques similar to those believed to occur within the human mind to perform observable, high-level functions of the mind (e.g., face recognition using convolutional neural networks); or
b. a more general, inclusive approach that requires intelligence of function but disregards the means of implementation within the system (e.g., face recognition systems of any type); or
c. any processing conducted, regardless of the scale, purpose or function of that computation, that contains an element of AI (e.g., the use of machine learning, neural networks etc. for any internal function of a system that may not necessarily outwardly exhibit intelligence to the user during operation); or
d. any machine either performing intelligent high-level functions or performing intelligent internal computation – i.e., any system satisfying either b or c above (e.g., when indicating a range of systems that might be considered AI).

For some users of the term AI, specific restrictions are intended (sometimes only by implication) in certain circumstances. Consider a biometric engine trained using AI processes – but otherwise not using AI in day-to-day operations. It might be claimed that such an engine does not use AI [i.e., limited in meaning to 'in production'], for fear of implying that its operations may change uncontrollably over time.

1.2 Biometrics as a branch or instance of AI

Example: AI activities that include machine-performed recognition of individuals as one such activity and thereby presenting biometrics as a subset of AI technologies.

1.3 Biometric algorithms enhanced by substituting AI techniques for matching

Example: Using AI techniques to determine identity or attributes of a person which could otherwise have been determined using other biometric processing techniques.
Example: Face recognition systems began using machine learning to dramatically improve performance ca. 2018.
NB 'matching' means 'the means by which a biometric system compares characteristics of one person with those of other people'.
NB both senses of 'algorithm' outlined in the Institute's *Explanatory Dictionary of Biometrics* apply here – AI can be used in sub-components or as a component of the system as a whole.

1.4 Biometric algorithms trained using AI functions

Example: Face recognition algorithm trained by using a dataset of images, generated by an AI tool, to cover particular demographic groups, poses etc.
NB this is the same AI tool that can also be used to create a false biometric identity - see 'Creation of a fake identity' using AI below.

2. What is the scope for the use of AI in biometric applications?

2.1 Representation of another person generated using AI

Example: Video generation of a seemingly real video footage of another known person in order to impersonate them, whether for human consumption, or at the time of biometric enrolment or verification.
NB the term 'deepfake' is often used to describe such generated media. It is unclear whether that term would be applied to non-human-visible representations (say, an AI-generated replica of palm vein geometry).

2.2 Creation of a fake identity using AI

Example: Creation of imagery / attributes of an entirely new person to present to the biometric engine in order to conceal his/her true identity.

2.3 Creation of synthetic 'merged person' using AI (morphing)

Example: Creation of biometric imagery /attributes that combine key features of several real people to present to the biometric engine, often in an attempt to allow several people access to the same identity document/resources/location

2.4 Indirect attack through diminishing other defences

Example: Using AI to break other security protocols, leaving only the biometric elements providing defence against attack and therefore magnifying any imperfect performance characteristics inherent within the system.

2.5 Biometrics protected using AI - Detection of real person

Example: AI techniques used to determine whether the person(s) present in video footage is real or not before employing biometric face recognition technology (to mitigate 'deep fakes,' whether human- or AI-generated; or the use of a mask or other facial occlusions/fabrications by a human attacker).

2.6 Monitoring usage for fraud

Example: AI determining whether a presented fingerprint biometric is from the user of a terminal rather than another party or a fake fingerprint presentation [e.g. using camera footage]

2.7 Biometrics used alongside other AI - Assembly of several human-like functions to perform tasks

Example: A serving robot combining face recognition with speech recognition and language comprehension to take orders and return correct items to the right person
Example: Use of biometrics and activity detection to determine what individuals are doing and/or whether they are compliant with rules in a particular location

3. What are the corresponding issues between AI and biometrics?

3.1 Explainability

When and why would the AI process need to be explained?
Building and maintaining public confidence and trust in AI is critical if the technology is going to gain widespread acceptance as it expands and develops into many areas of society. Consequently, it is vital that the operation of AI systems and, by association, biometric applications can be explained clearly and effectively to everyone using or being affected by these technologies.
However, there are also some areas where the concept of explainability needs to be more specific and detailed, for example, in many criminal justice systems, operating under full disclosure principles, there is often a requirement for expert witnesses to explain to the court how they arrived at their conclusions, and this has traditionally included the use of biometric systems conducting search processes as part of a crime investigation. This has, in the past, been relatively straightforward to explain. However, the 'black box' nature of AI technologies, found in many modern biometric systems, means that those giving expert evidence may now be unable to satisfactorily describe how the biometric processing produced its outputs. This may not be relevant when the human expert(s) agrees with the findings contained in these outputs but when digital and human conclusions do not coincide this could potentially result in unsafe convictions or acquittals in court. Therefore, the traditional 'human in the loop' safeguard may not be viable, in the future, as the technology may begin to outperform human adjudication in some scenarios.

3.2 Requirements for data

Construction of AI systems requires examples of the data being processed, whether to inform human-led training or independent machine learning for the system, to underpin validation that the system performs its activities satisfactorily, or any of many other processes involved in system design and implementation assurance. This is true whether talking about AI as a functional output – e.g. machine detection of objects in a scene or recognition of individuals, or of AI as an internal procedure – e.g. machine learning by neural networks.

The sources, provenance, consent processes, alignment with target use cases, unintended bias and many other issues that can affect data sets apply similarly to both biometrics and AI more generally. In this regard, many of the challenges facing data sets for use in biometrics also apply to data sets for use in other AI systems.

3.3 Ethics

AI is an active technology that is capable of learning and improving its functions through processes such as machine learning and therefore it poses a unique challenge to the future of human endeavour and social structures. Deploying AI in an ethical manner is of paramount importance for civil society and many of the good practice guardrails, recommended by the Biometrics Institute, are equally applicable to AI (See the Institute's '*Ethical Principles for Biometrics*'). For instance, precision medicine is an emerging field of science that uses AI and the human genome to both predict, prevent and treat disease. However, the genome can also be used for a variety of other functions, both altruistic and oppressive, e.g. identity verification, genealogical and familial analysis, phenotypic typing, social grouping and repression, voluntary (and involuntary) screening for organ donation etc.

3.4 Community governance expectations

The emergence and rapid spread of artificial intelligence across many aspects of society has raised concerns regarding the impact of the technology on human agency and discretion and how this can be controlled effectively. Examples of this include:

- Strong and diverse views on the ethical use of both AI and biometric technologies.
- The role of human oversight in critical decision-making (see 'Explainability' above).
- Expectations of executive accountability and responsibility for, and oversight of, such technologies.
- A desire to minimise negative impacts of these technologies on particular groups of stakeholders and especially those who are most vulnerable.
- The potential for AI technology to perform tasks better than humans, and the consequences for our society, economy, legal system etc.
- Historically, man-made technologies have been passive in nature and controlled by humans. AI is an active technology and therefore not necessarily dependent on human control (e.g. generative AI platforms, autonomous civilian and military vehicles etc.) and this has fuelled debates, on an international scale, as to how the technologies can be effectively governed by humans in the future.

Supporting material

The output of this consultation will be a new entry to the Biometrics Institute Explanatory Dictionary for artificial intelligence. Please refer to the draft document for more information.

Contact

You are also welcome to write to us but we are only able to accept submissions that use the existing discussion paper and the accompanying draft of the "Explanatory Dictionary entry for artificial intelligence" and mark up proposed changes to those documents.

Biometrics Institute
manager@biometricsinstitute.org

Artificial Intelligence (AI) ⃠

Biometrics usage

1. A machine, system etc. that performs intelligent functions or processes data using mechanisms believed to underpin intelligence (e.g., machine learning); or describing such a system.

   Many use AI to mean 'both performing intelligent function and containing intelligent data processing'. However, sometimes only one of these is intended; and sometimes systems with either function or processing are included (often when describing several such systems). Consequently, the meaning is often not obvious from the context; see examples 1, 2a and 2b below for illustration. Especially in formal use, ensure that the intended meaning is clear.

   This inconsistency confounds the relationship between biometrics and AI. Some view that all biometric systems are AI – applying to AI only an 'intelligence of function' requirement. Others argue that biometrics are only AI if they use intelligent data processing such as machine learning and neural networks.

2. AI has been increasingly employed in mainstream biometric processing in recent years, but it also features in other aspects of these applications:

   a) **AI attacks on biometric systems -** Threats from AI technologies that can seriously impact biometric applications are ever-present and growing. These include elements such as 'deep fakes' (where a person's face or voice is impersonated with AI techniques) and more general AI cyber attacks which result in the corruption or loss of data within the system.
   b) **AI protecting biometric systems -** AI can also play a crucial role in countering these threats by detecting incoming attacks and analysing and quality assuring data integrity.

More information is available in the paper *'The Relationship Between Biometrics and AI'* (see above) which explores this topic further.

Context and wider usage

In very general terms AI may be considered to be any form of an autonomous or partially autonomous computing system that is able to:

1. Simulate human thought, learning or behaviour.
2. Analyse large data sets to classify material, solve problems and make decisions, predictions or recommendations that previously would have required human intelligence.
3. Process data on a scale that exceeds human abilities.

However, it should be noted that many stakeholders observe the difficulty of drafting a solid definition for AI.

Confounding factors include:

- Interest in AI from a wide array of governing bodies, commentators, and the public.
- Lack of clarity and shifting perspectives over time on what does and does not constitute 'intelligence' either in function or computation; and therefore what AI is when compared to non-intelligent machines.
- Reliance on comparisons with human intelligence. While analogy can aid understanding, it can lead to 'things that previously required human intelligence'. 50 years ago, that was true of calculators – yet we do not now consider calculators to contain AI technology.
- Different stakeholders desire different entities to be considered, or not considered, as AI and even these predilections sometimes change over time.

Examples

1.

- The AI technology in the cameras recognised people passing in the street and presented them with tailored advertising on the electronic hoardings.
- Regulators are concerned about the non-consensual public capture and processing of face images using artificial intelligence facial recognition technology.

(NB these examples may well use techniques such as convolutional neural networks, but do not need to; and the actions and concerns described do not depend on this.)

- Face recognition system performance improved circa 2018 by adding AI (implying that prior to that time, non-AI algorithms were used).
- The legislators sought to impose controls on all types of AI systems (NB how would the scope of this intended action be defined?).

2a. Audio presented to the voice recognition system was actually an artificial intelligence-generated 'deep fake'. (NB that 'deep fake' usually implies generation by neural network techniques.)

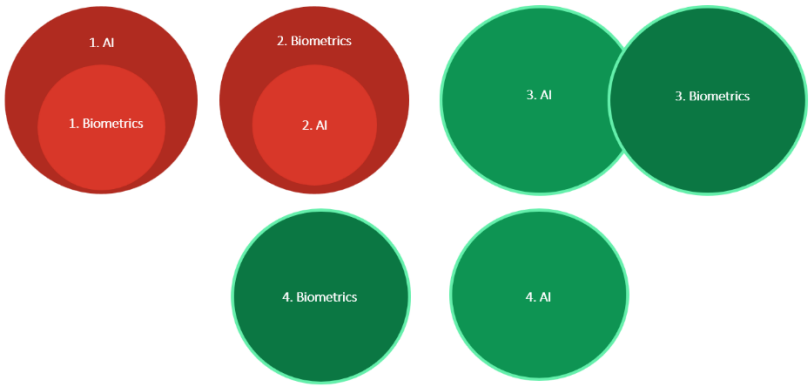
2b. The attempt to enrol an altered, imposter's face image into the biometric system was prevented by artificial intelligence software that detected spurious artefacts and small distortions in the features. (NB a good example of where the process described may refer to a specific AI technique or be open to a wider interpretation i.e. any such software would be AI, no matter how implemented?).

Definitions in technical use

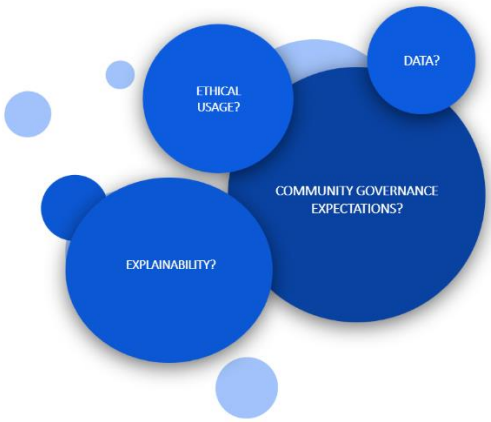
Russell & Norvig – 'Systems that act/think like humans,' aligned with the function/processing split noted in definition 1.
Google – Alternative - either intelligent in both function and processing as in definition 1; or using data analysis beyond human scale (Wider usage no.3).
US Presidential order – Intelligence in both function and processing.
EU AI Act (and OECD) – Intelligence in both function and processing.
ISO – Intelligence in either function or processing.
NIST CSRC – Intelligence in processing only.

Annex: Powerpoint presentation highlighting key questions

How would you define the relationship between AI and biometrics?



Biometrics & AI: What are the corresponding issues?



How does AI interact with biometrics?